1.0 INTRODUCTION

1.0 INTRODUCTION

1.1 DESCRIPTION

This section of the *Nlets User and Technical Guide* presents pertinent information regarding the background of Nlets, the use of the system, and the use of this Guide. The reader should be familiar with this section of the Guide before attempting to interface with, or otherwise use, the Nlets automated system.

1.2 NLETS ORGANIZATION

1.2.1 ADMINISTRATION

Nlets, the International Justice and Public Safety Network is made up of representatives of law enforcement agencies from each of the 50 states, the District of Columbia, Puerto Rico, U.S. Virgin Islands, many Federal law enforcement agencies and the National Insurance Crime Bureau (NICB). There is also a connection to the Canadian Police Information Centre (CPIC). Nlets is incorporated under the laws of the State of Delaware and is a non-profit organization whose purpose is to provide interstate communications to law enforcement, criminal justice and other agencies involved in enforcement of laws.

Organizationally, Nlets is comprised of eight regions. Each region represents six or seven states and several federal agencies that are grouped together to represent a regional community of interest.

The chief executive office of each Control Service Agency for a state or other member agency shall appoint an individual to provide representation in the Nlets organization. The state representatives of each region elect a Chairman and a Vice-Chairman each year. The Chairman represents the region on the Nlets Board of Directors.

The Board of Directors meets at least once each year to conduct the organization's business. All policy decisions are made by the Board of Directors. The policy decisions range from how the system is to be operated to how the Corporation's general business will be handled.

The Nlets state representatives elect a President, First Vice-President, and Second Vice-President for a two year term. The President serves as Chairman of the Board at all Board and Council Meetings.

The Board of Directors appoints an Executive Director who is responsible for conducting the organization's day-to-day business and to see that the Board's decisions on system operational and administrative matters are carried out.

Executive Director's Office

1918 Whispering Wind

Phoenix, Arizona 85016

Nlets Office telephone number: 623-308-3500

Nlets website link: http://www.nlets.org

1.2.2 FINANCIAL

Each Nlets member must pay the prevailing service charges. For states, this fee relates to the number of members involved rather than the direct cost per state. There are special billing policies for other members depending on how they are interfaced to the system. These policies may include billing for actual circuit costs and/or a levy based on the number of terminals being serviced.

1.2.3 NLETS CONTACTS

Personnel requiring information or assistance of an operational or emergency nature, they may contact the 24-hour operations center at 800-528-4020 or via Administrative message to ORI/AZNLETS20.

Personnel needing any other assistance may find a comprehensive list of Nlets personnel and job functions, complete with phone numbers email addresses on the Nlets website: at http://www.nlets.org.

.

1.3 DESCRIPTION OF NLETS

Nlets' sole purpose is to provide for the interstate and/or interagency exchange of criminal justice and criminal justice related information.

The mission of Nlets is to provide, within a secure environment, an international criminal justice telecommunications capability that will benefit, to the highest degree, the safety, security, and preservation of human life and the protection of property. Nlets will assist those national and international governmental agencies and other organizations with similar missions who enforce or aid in enforcing local, state, federal or international laws or ordinances.

Technically speaking, Nlets is a sophisticated message switching system linking local, state, and federal agencies together to provide the capability to exchange criminal justice and public safety related information by means of computers, terminals, and communication lines. Nlets links the state computers together via high speed frame relay circuits. Using this concept coupled with a standardized nationwide addressing scheme, a local agency may transmit and receive from another agency outside his or her state in a matter of seconds.

13.1 POINT OF ENTRY

Each state has a point of entry. This is the location where the Nlets line actually terminates. The POE will is the state computer system that interfaces with the Nlets computer. The POE is not to be confused with the Control Service Agency. The POE is responsible for the actual maintenance of the interface. This includes coordinating modifications, installing new equipment, and notifying Nlets of out of service situations, planned or unplanned.

1.3.2 CONTROL SERVICE

Each Nlets member must designate an agency as the **Nlets System Agency (NSA**). This designated agency is responsible for maintaining operational surveillance over the state end of the line and for providing distribution services in and out of the Nlets network. The NSA is normally addressed by using the two-character ORI (state code) xxNlets00 where xx = state code.

Traffic is directed automatically to the destination ORI(s) on the state network. The NSA is responsible for the expeditious delivery of messages to the designated destination ORI. An exception to this rule is the distribution of statewide broadcast messages

Furthermore, no information delivered from Nlets is to be used for any purposes other than that for which it was originally requested. Exceptions to this rule allow:

- The review of message traffic for quality control.
- The usage of traffic for statistical analysis purposes.

1.3.3 MESSAGE ROUTING

All messages must be routed using the appropriate NCIC Originating Agency Identification (ORI) code or an Nlets authorized ORI. Detailed rules for ORIs may be found in Message Structure Section of this manual. Nlets checks the ORI for incoming traffic and sends messages directly to the proper state point of entry. Any detected errors are returned to the sending terminal by the Nlets computer or the state POE. Inquiries are routed to the state(s) designated in the message. It is then the state's responsibility to handle the inquiry and to return the appropriate response as quickly as possible.

1.3.4 MESSAGE FORMAT

Messages can be formatted either in eXtensible Markup Language (XML) or in the Nlets native text format.

1.3.4.1 OVERVIEW

Nlets allows NSAs to format messages in eXtensible Markup Language (XML) then send and receive those messages via the National Justice Information Network (NJIN). When an XML message is sent, the Nlets NJIN converts the XML into native text format conforming to Nlets standards and the same process occurs in reverse when a response is received. Messages formatted in XML must be according to the XML specifications discussed in this Guide.

The Nlets NJIN must be used to transition state NSAs from Nlets TCP/IP socket protocol with native Nlets text messages to Web services with XML formatted messages. The Nlets NJIN allows great flexibility with regard to message routing, protocol bridging and format conversion. Therefore when utilizing the Nlets NJIN, a state NSA has the option of transitioning any message types to Web services and XML, while maintaining native transport and format for other message types. Further, a state NSA can convert any number of state ORIs to Web services, while maintaining native transport and format for other ORIs. The Nlets NJIN will store all message transaction in an XML storage type that will not only provide a structured data representation, but also ensure the preservation of the Nlets native text format.

1.3.4.1.1 XML FORMAT

XML (eXtensible Markup Language) is a flexible markup language which can be used to define any type of structured information and pass that information between different computing systems, regardless of their architecture. XML is a non-proprietary standard maintained by the World Wide Web Consortium (W3C).

1.3.4.1.2 NATIVE NLETS FORMAT

When a message format differs from state formats, and they are not produced in XML, each state must reformat to conform to Nlets standards and the following rules should be observed:

All formats for message headers, control characters, inquiries, control/status messages, and error messages are fixed.

Trailing spaces in each data field should not be in fixed format messages to Nlets. For example if the name field can hold a maximum of 30 characters, but if the name submitted is only 15 characters, the state should remove the trailing 15 spaces.

1.3.5 MESSAGE RETENTION

Nlets receives, stores, and forwards messages. In the event that a destination POE is able to receive, messages are sent immediately. If the receiving POE is inoperable, the sending terminal is notified the destination is temporarily out of service. Nlets sends an APB message when a user is experiencing a large outage, then sends another when the user is back in service.

Normally, all messages are held on queue until the receiving state is back in service. However, if a user is going to be down for an extended period, they may request to be placed on **"remove"** status. This means that messages sent to that user will not be stored. Rather, they will be returned to the sender with a notification that the user is down. The message must then be resent after the sender is notified that the destination has returned to service.

1.3.6 COMPUTER INTERFACE WITH STATE NETWORK

Nlets uses permanent virtual circuits (PVCs) over a private frame relay network to communicate with state networks. The Transmission Control Protocol/Internet Protocol (TCP/IP) is used as the communications protocol for all communications over the network. Cisco routers provide the IP network services and perform router-to-router triple DES encryption.

Nlets supports the following three interface protocols: Web Services, IBM's proprietary WebSphere® MQ messaging and Nlets TCP/IP Socket Protocol (NTP)

1.3.6.1 WEB SERVICES

The Nlets NJIN provides support for industry standard Web services. Web services provides for the definition, discovery, and transmission of data, typically in XML format. Web services are composed of four standards:

- XML for data format
- Simple Object Access Protocol (SOAP) for data transfer
- Web Services Definition Language (WSDL) for interface definition
- Universal Description, Discovery, and Integration (UDDI) for service discovery

Nlets provided support for a Web services interface to enable state NSAs to transition Nlets connections to open standards. Nlets Web services interface will enable members to deploy XML capable solutions that leverage the many standards initiatives, including the Rap Sheet XML standardization. In addition Nlets Web services will provide Nlets members with improved functionality, for example support for attachments.

1.3.6.2 WEBSPHERE® MQ

The Nlets NJIN also provides support for IBM WebSphere® MQ. The Nlets NJIN provides Nlets members with the option of exchanging message transactions using a message queue interface. The Nlets NJIN MQ interface expands the interface options by enabling assured one-time delivery, time independent communication, and support for high volume message queues.

In addition, the Nlets NJIN MQ interface provides support for ***both*** Nlets native text format ***and*** Nlets XML format. Thus, the Nlets NJIN will provide the necessary message format conversion before forwarding the message throughout the Nlets message system.

It should be noted WebSphere® and XML capabilities are NOT bundled together and therefore can be deployed separately.

Refer to Appendix E for a detailed message queue specification and complete information on transitioning a state NSA to the Nlets NJIN message queue interface.

1.3.6.3 NLETS TCP/IP SOCKET PROTOCOL

Nlets TCP/IP Socket Protocol received that name because it was the first protocol used by Nlets which operated using the TCP/IP protocol. Nlets TCP/IP Protocol is actually a specialized exchange protocol, which operates using the TCP/IP protocol. Nearly all communications protocols use TCP/IP as the underlying transport protocols. NSP provides for the exchange of messages using up to eight TCP/IP sessions in a send/acknowledge lock step fashion. A heartbeat is used to detect an outage. Appendix D provides the detailed specification for this protocol.

1.3.7 AUTOMATED INTERFACE WITH STATE NETWORK

All states interface with Nlets via a computer-to-computer interface. This allows states to use varied formats, depending upon the state requirements and the particular terminal and computer network within that state. Many of the specific operations of Nlets will be transparent to local users in the states. Differences in formats and types of terminals will be resolved in the state computer program that supports the Nlets interface.

1.3.8 EXTENDED ROUTING (ORI MANIPULATIONS AND CONTROL FIELD)

The first seven characters of the NCIC assigned ORI provide a unique address for each law enforcement agency in the United States. The identification of precincts, substations, or other terminal locations within a single agency may be provided for by assigning specific numbers as the last two characters of the ORI. By providing this level of definition, the NCIC ORI code can be used to identify and address individual terminals on the state system or on computer systems within a state such as county or metropolitan systems.

There may be instances where use of the last two characters of the standard ORI is insufficient to uniquely identify a terminal. In these cases the user may contact NCIC to determine whether they qualify for an additional ORI for their agency.

An additional routing capability allows agencies from Federal members (ATF, DEA, IRS, etc.) without a direct interface to Nlets, to obtain terminals on state systems and use these terminals to access Nlets. This is accomplished by placing an "S" in the 8th position of the agency's ORI. This "S" will allow this terminal to access Nlets through the state system while also allowing other terminals from the same agency to access Nlets through their Federal Member system, e.g. DOJ.

When sending a message to a terminal on the Department of Treasury (TECS) System, the National Crime Information Center (NCIC) or any other Federal user, it should be addressed to the assigned ORI as found in the ORION file. No special addressing techniques are required for point-to-point messages.

1.4 NLETS USERS AND USES

The success of the system depends upon enforcing Nlets polices that control who uses the network and for what authorized purposes. Although Nlets is responsible for development of policy, the Nlets members carry the burden for assuring that all Nlets policies and regulations in this regard are followed.

1.4.1 TYPES OF USERS

Nlets is a criminal justice system. Only criminal justice agencies and those non-criminal justice agencies that, through their participation, provide a benefit to public safety or the law enforcement/criminal justice community are authorized to participate on Nlets.

The following table lists agencies and organizations authorized to participate on Nlets along with any special restrictions. Some agencies, or classes of agencies, may appear (be authorized) more than once depending upon if they serve multiple functions.

Types of Users	***Special Restrictions***
Non-federal criminal justice agencies in each state, the District of Columbia, Puerto Rico, and the Virgin Islands	ORI must be assigned by NCIC. No restrictions.
Federal criminal justice agencies	ORI must be assigned by NCIC. No restrictions.
Non-government agencies: • National Insurance Crime Bureau (NICB) • National Center for Missing & Exploited Children (NCMEC)	No CHRI access (Message types IQ/IR, FQ/FR, AQ/AR, and CR prohibited.) See agreements for further details.
Agencies authorized under **PL99-169** for national security purposes: • Central Intelligence Agency (CIA) • Office of Personnel Management (OPM) • Defense Investigative Service (DIS) • National Security Agency (NSA) • Federal Bureau of Investigation (FBI)	Access for National Security Purposes ORI must be assigned by NCIC. **PL99-169** "The Intelligence Authorization Act of Fiscal Year 1986", Title VIII, Section 910 (entitled “Access of Criminal History Records for National Security Purposes").
Government agencies authorized under state or Federal statute to investigate, respond to, regulate, clean up or evacuate as a result of chemical, hazardous material, or an incendiary incident. This also includes state and local emergency management offices.	Weather files (HQ/HR) and AM access in emergency situations. Must have “H” or an “S” in the 9th character of the ORI. or Must have an NCIC assigned ORI.

Types of Users	Special Restrictions
State governmental agencies responsible for the licensing of driver and registration and/or titling of vehicles and related enforcement activities.	No CHRI Access (Message types IQ/IR, FQ/FR, AQ/AR, and CR prohibited.) This does not preclude the exchange of driver registration and/or history information by DMV's. ORI must end in a "V" and be assigned by NCIC or end in an "S".
Criminal Justice agencies in Canada	ORI must be assigned by RCMP. No restrictions.
Police Departments: • Police Departments authorized by state statute but maintained by private colleges or universities. • Railroad police	Full access provided. NCIC ORI ends in "E".
Communications centers set up to provide service to police and fire departments, and other local government agencies (i.e., "911" centers).	No CHRI access when there is a "P" in 9th character of the NCIC ORI.
Governmental agencies responsible for enforcing laws or ordinances	ORI must be assigned by NCIC or end in an "S" and be assigned by Nlets. If assigned by Nlets the agency is restricted from requesting CHRI and cannot use Nlets for licensing or employment purposes.
Civil Courts when seeking criminal history information pursuant to the Violent Crime and Law Enforcement Act of 1994 for use when hearing civil domestic violence or stalking cases.	ORI must be assigned by NCIC and end in a "D". Purpose code must be "D".
National Weather Bureau	May only send "AM" to criminal justice agencies regarding road/weather information when multiple states are involved.
HUD agencies assigned a "Q" ORI	May only receive criminal history information using a "CR" message type (a response from a Triple I inquiry). The "Q" ORI must be assigned by NCIC.

All Nlets NSAs are responsible for assuring that any agencies that they provide Nlets access to are included in the table above. When a criminal justice agency performs a service on behalf of a governmental non-criminal justice agency, each agency must have an ORI. In all transactions the ORI of the governmental non-criminal justice agency must be used.

If the non-criminal justice agency does not have an ORI and is using Nlets for approved purposes, we will assign an Nlets ORI. This is the "S" ORI.

If the non-criminal justice agency contracts with a private firm, there must be an agreement signed by a representative from the non-criminal justice agency, the private contractor and the Nlets representative. This agreement guarantees that the non-criminal justice agency will assure that Nlets policies and procedures are followed by the private contractor.

1.4.2 STATE/USER RESPONSIBILITIES

Each state (member) is responsible for providing an interface with Nlets, thereby providing access for all criminal justice agencies or other authorized agencies in the membership to all other criminal justice or other authorized agencies in the nation. With this responsibility, the member has the authority, and must exercise the authority, to insure that all users provided access by the member follow the Nlets policies, especially those relating to security of the system and security of the information transmitted on the system.

Failure of the agencies within the member state or agency to follow the proper procedures must be called to the attention of the Nlets Control Service officer who will in turn take corrective action with the originating agency. Continued violations must be reported to the Nlets Board of Directors for further action.

1.4.3 MAINTENANCE

Nlets' equipment or line problems are to be reported to the Nlets Control Center by the user agency. The Nlets Control Center will then coordinate all trouble isolation. Costs associated with network maintenance are included in the Nlets membership fees.

1.4.4 GENERAL SYSTEM USAGE

All traffic over the system must be in the prescribed message form. Unnecessary messages with superfluous verbiage or embellishments are prohibited. Information of no value to the addressee must be avoided. For example, address or telephone number of parents reporting runaway children are of no value to another department who will notify the originating department, not the parents, of any apprehension. Avoid expressions such as "ARREST AND HOLD", "HOLD FOR INVESTIGATION", "HOLD AND NOTIFY", "DETAIN FOR THIS DEPARTMENT", "WANTED AS SUSPECT", etc.

The name of the crime should be clearly specified and if a warrant has or will be issued. If a warrant has been issued it should be in the NCIC system.

In view of the many persons who may receive messages, the use of non-standard abbreviations must be avoided. Keep in mind that many abbreviations that may be in common use within one department or in one state may be entirely unknown and confusing to another department or state.

It is imperative that departments originating want messages of any type cancel these messages when they no longer apply. Messages may be canceled only by the originating department. Departments apprehending a wanted subject or recovering a stolen or wanted vehicle should direct a message to the originating station only, reporting the apprehension or recovery. The originating department should then cancel their outstanding messages and clear their NCIC file entry.

1.4.5 RESTRICTIONS

The system must not be used for the following types of messages:

- No social announcements, i.e., Christmas messages, retirements or convention notices.
- No recruiting of personnel.
- No messages in which the complainant is interested only in the recovery of property.
- No attempts to locate vehicle (breach of trust) without warrant. For the protection of the arresting officer, messages should not be dispatched until a warrant is secured.
- No excessively long messages.
- No transmission of subpoenas.
- Use of vehicle registration and driver license information obtained via Nlets is limited to a criminal justice purpose.
- Automated positive message acknowledgment (PMA) will not be allowed except when a need can be shown that automated PMA is required in order to capture information that can be of substantial value in diagnosing an information exchange problem. Under no circumstances will the temporary use of PMA exceed 45 days. Authorization for temporary PMA can be given by the Executive Director.
- No solicitation of funds.

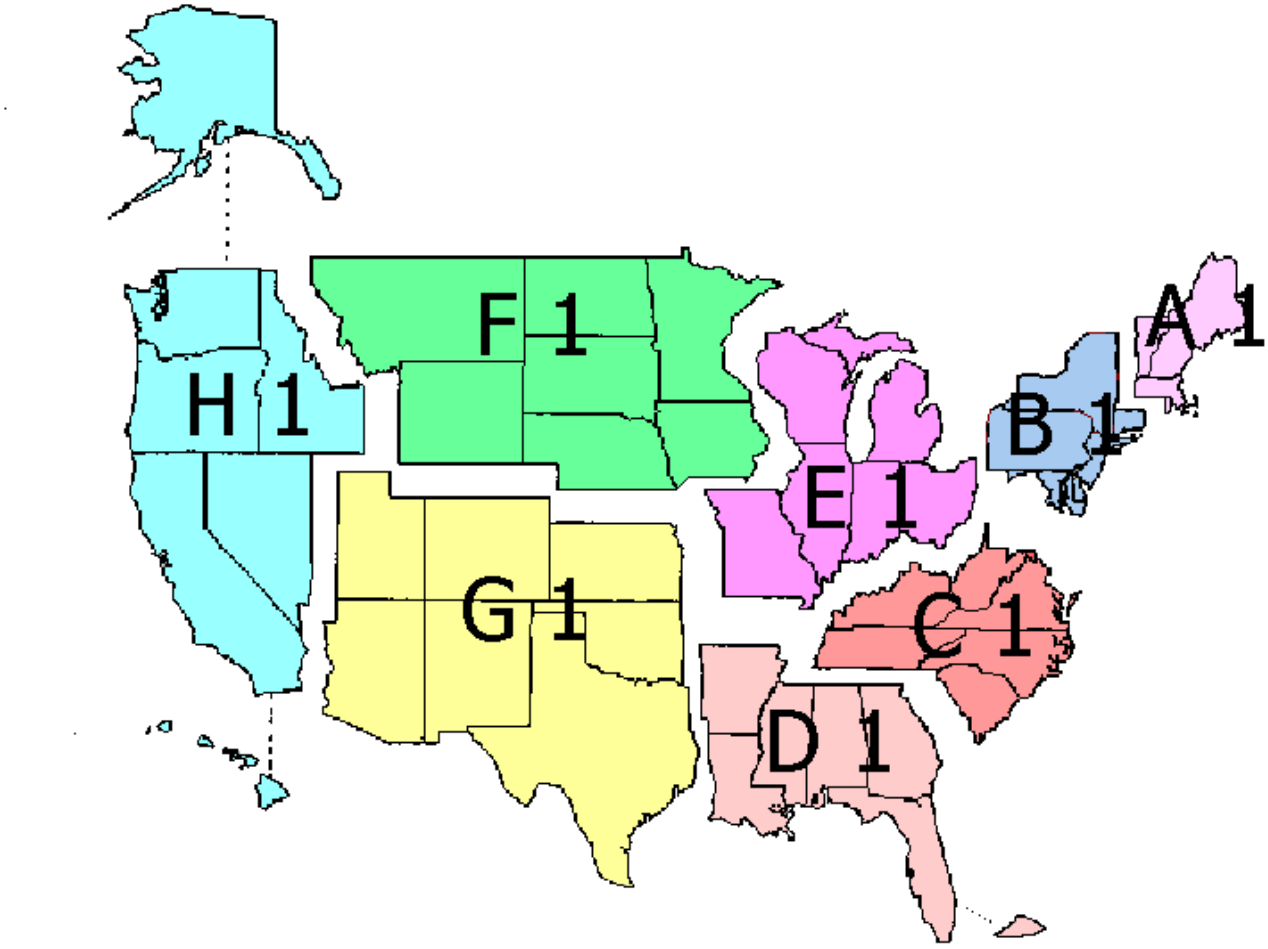
1.5 ADMINISTRATIVE DOCUMENTS

A number of administrative documents and forms are required for both member and non-member entities.

If an entity is unable to locate their original signed documents, the Nlets administrative staff can provide copies of these documents.

1.6 NLETS REGIONAL MAP

Nlets is comprised of eight regions. Each region represents six to seven states and several federal agencies that are grouped together to represent a regional community of interest.



Region A (Code: "A1")	*Region B (Code: "B1")*	*Region C (CODE: "C1")*	*Region D (CODE: "D1")*
Connecticut	Delaware	Kentucky	Alabama
Maine	District of Columbia PD	North Carolina	Arkansas
Massachusetts	Maryland	South Carolina	Florida
New Hampshire	New Jersey	Tennessee	Georgia
Rhode Island	New York	Virginia	Louisiana
Vermont	Pennsylvania	West Virginia	Mississippi
Air Force OSI	FBI/NCIC	Department of Justice	Puerto Rico
Department of State	Postal Service	Nat'l Sheriff's Association	INTERPOL
Naval Investigative Service	U.S. Secret Service	Postal Inspection Service	American Samoa
FBI	Nat'l Center for Missing	FBI	FBI
Postal Service	& Exploited Children	Postal Service	Postal Service
Region E (Code "E1")	***Region F (CODE "F1")***	***Region G (CODE "G1")***	***Region H (CODE "H1")***
Illinois	Iowa	Arizona	Alaska
Indiana	Minnesota	Colorado	California
Michigan	Montana	Kansas	Hawaii
Missouri	Nebraska	New Mexico	Idaho
Ohio	North Dakota	Oklahoma	Nevada
Wisconsin	South Dakota	Texas	Oregon
N.I.C.B.	Wyoming	Utah	Washington
FBI	Dept. of the Army	Department of the Interior	ICE
Postal Service	FBI	FBI	FBI
	Postal Service	Postal Service	Postal Service